SUPREME COURT OF NEW JERSEY
DOCKET NO. 82209
Appeal No. A-72-18

STATE OF NEW JERSEY, Plaintiff-Appellee v. Robert ANDREWS, Defendant-Appellant	Criminal Action On Appeal from a Final Order of the Superior Court, Appellate Division, Affirming the Interlocutory Order of Superior Court of New Jersey, Law Division, Essex County, Indictment No. 16-06-1781 Sat Below: Hon. Joseph L. Yannotti, PJAD Hon. Garry S. Rothstadt, JAD Hon. Arnold L. Natali, Jr., JAD

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER

On the brief:
Frank L. Corrado
Marc Rotenberg
Alan Butler
Megan Iorio

FRANK L. CORRADO
Barry, Corrado, Grassi & Gillin-Schwartz, P.C.
2700 Pacific Avenue
Wildwood, NJ 08260
(609) 729-1333
Counsel of Record for Proposed Amicus Curiae Electronic Privacy Information Center

ALAN BUTLER (*PHV Pending)
MEGAN IORIO (*PHV Pending)
Electronic Privacy Information Center
1718 Connecticut Ave NW
Suite 200
Washington, DC 20009
(202) 483-1140

TABLE OF CONTENTS

TABLE OF CONTENTS I

TABLE OF AUTHORITIES II

INTEREST OF AMICUS 1

PRELIMINARY STATEMENT 3

ARGUMENT 5

I. CELL PHONES PROVIDE ACCESS TO A VAST AMOUNT OF INFORMATION THAT LAW ENFORCEMENT PREVIOUSLY HAD TO EXPEND SUBSTANTIAL RESOURCES TO IDENTIFY AND LOCATE. 5

II. RECENT U.S. SUPREME COURT DECISIONS CONCERNING PRIVACY PROTECTIONS FOR CELL PHONES COUNSEL IN FAVOR OF A NARROW APPLICATION OF THE FIFTH AMENDMENT FOREGONE CONCLUSION EXCEPTION. 16

A. IN RILEY V. CALIFORNIA AND CARPENTER V. UNITED STATES, THE U.S. SUPREME COURT SIGNALED THAT COURTS SHOULD PRESERVE CONSTITUTIONAL PROTECTIONS, AND NARROW EXCEPTIONS, FOR CELL PHONE DATA. 18

B. A BROAD INTERPRETATION OF THE FOREGONE CONCLUSION EXCEPTION AS APPLIED TO CELL PHONES WOULD SIGNIFICANTLY UNDERMINE FIFTH AMENDMENT PROTECTIONS. 20

CONCLUSION 25

TABLE OF AUTHORITIES

CASES

Carpenter v. United States,
138 S. Ct. 2206 (2018).....passim

Commonwealth v. Baust,
89 Va. Cir. 267 (Va. Cir. Ct. 2014).....24

Commonwealth v. Davis,
176 A.3d 869 (Pa. Super. Ct. 2017).....23

Commonwealth v. Jones,
117 N.E. 3d 702 (Mass. 2019).....23

Doe v. United States,
487 U.S. 201 (1988).....16

Fisher v. United States,
425 U.S. 391 (1976).....4, 21

G.A.Q.L. v. State,
257 So. 3d 1058 (Fla. Dist. Ct. App. 2018).....24

In re Application for a Search Warrant,
236 F. Supp. 3d 1066 (N.D. Ill. 2017).....5, 24, 25

In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011,
670 F.3d 1335 (11th Cir. 2012).....23

In re Search of a Residence in Oakland,
354 F. Supp. 3d. 1010 (N.D. Cal. 2019).....25

Riley v. California,
573 U.S. 373 (2014).....passim

Schmerber v. California,
384 U.S. 757 (1966).....16, 20, 21
Smith v. Maryland,
442 U.S. 735 (1979).....19
State v. Stahl,
206 So. 3d 124 (Fla. Dist. Ct. App. 2016).....23
United States v. Apple Mac Pro Computer,
851 F.3d 238 (3d Cir. 2017).....23
United States v. Dionisio,
410 U.S. 1 (1973).....16
United States v. Fricosu,
841 F. Supp. 2d 1232 (D. Colo. 2012).....23
United States v. Hubbell,
530 U.S. 27 (2000).....4, 21, 22
United States v. Mitchell,
76 M.J. 413 (C.A.A.F. 2017).....23
United States v. Wade,
388 U.S. 218 (1967).....24

CONSTITUTIONAL PROVISIONS

U.S. Const. amend. V 21

OTHER AUTHORITIES

Accengage, 2018 Push Notification Benchmark (2018) 13

Alex Young, Can I Control My Home Security from My Phone, Safewise (May 17, 2019).....15
Alexandra Chang, Your Door is About to Get Clever: 5 Smart Locks Compared, Wired (June 19, 2013).....15
Andrew Martonik, Let's Be Honest, 64GB of Internal Storage is Plenty in 2018, Android Central (Feb. 2, 2018).....6
Andrew Perrin & Monica Anderson, Share of U.S. Adults Using Social Media, Including Facebook, Is Mostly Unchanged Since 2018, Pew Research Ctr. (Apr. 10, 2019).....11
App Annie, The State of Mobile 2019 (2019) 8
Apperian, Executive Enterprise Mobility Report (2016) 12
Apple, About Storage on Your Device and in iCloud (Sep. 27, 2018).....7
Apple, Empower Your Patients with Health Records on iPhone (2019).....10
Apple, Set Up iCloud Keychain (2019) 13
Bruce Schneider and Orin Kerr, Encryption Workarounds, 106 Geo. L.J. 989 (2018).....23
Caroline Cakebread, Who's Mobile Banking in the US?, eMarketer (Dec. 6, 2018).....9
Dashlane, Features (2019) 13
Dave Chaffey, Mobile Marketing Statistics Compilation, Smart Insights (July 11, 2018).....8
Diane Garey, BYOD and Mobile Security, Tenable (Apr. 5, 2016) .12

Eric Griffith, Two-Factor Authentication: Who Has It and How to Set It Up, PCMag (Mar. 11, 2019).....15

Ethan Jakob Craft & George P. Slefo, Mary Meeker's 2019 Internet Trends Report, AdAge (June 11, 2019).....7, 11

Facebook, How do I Log Out of the iPhone or iPad App? (2019) ..14

Google Nest Help, How to Control Your Nest Thermostat With the App (2019).....15

Hal Abelson, Hen Ledeen, & Harry Lewis, Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion (2008) 8

iClick, How Big is a Gig? (2013) 7

Ingrid Lunden, App Store Hits 20M Registered Developers and $100B in Revenues, 500M Visitors Per Week, TechCrunch (June 4, 2018).....9

Irene Rufferty, 50 Texting Statistics That Can Quench Everyone's Curiosity, Even Mine, Medium (Sept. 20, 2017).....10, 11

J. Clement, Average Daily Usage Frequency Per App in U.S. 2018, Statista (Aug. 14, 2018).....8

J. Clement, E-Mail Usage in the United States, Statista (Oct. 23, 2018).....10

John R. Delaney, The Best Smart Locks for 2019, PCMag (July 1, 2019).....15

Jonathan Garro, Unlock the Power of Your Mac's Keychain Utility, Tuts+ (Apr. 15, 2013).....14

Kim Zetter, How Thieves Can Hack and Disable Your Home Alarm System, Wired (July 23, 2014).....16

LastPass, LastPass Mobile (2019) 13

Matej Mikulic, Apple App Store: Number of Available Medical Apps as of Q1 2019, Statista (May 6, 2019).....9

Paul Krebs & Dustin Duncan, Health App Use Among US Mobile Phone Owners: A National Survey, 3 JMIR mHealth and uHealth (2015)..9

Pew Research Center, Mobile Fact Sheet (June 12, 2019) 4, 6

Sam Byford, Samsung is Making 1TB Storage Chips for Phones, The Verge (Jan. 30, 2019).....7

SmartHome, Control Lights With Your Phone (2019); Apple, Set Up and Use the Home App (2019).....15

Steelcase, Engagement and the Global Workplace (2016) 12

Syntonic, BYOD Usage in the Enterprise (2016) 11

Twitter, How to Log Out of the Twitter App on an iOS Device (2019).....14

Zack Whittaker, Facebook Admits It Stored "Hundreds of Millions" of Account Passwords In Plaintext, TechCrunch (Mar. 21, 2019) 14

Zoho Vault, Store and Organize Passwords (2019) 13

INTEREST OF AMICUS

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other Constitutional values.[1]

EPIC routinely participates as amicus curiae in cases concerning the application of constitutional protections to new technologies. EPIC has participated as amicus curiae before this Court. See, e.g., Brief for EPIC as Amicus Curiae Supporting Appellant, State v. Earls, 214 N.J. 564 (2013) (No. 68765) (arguing that individuals have a reasonable expectation of privacy in the current location of their cell phones); Brief for EPIC as Amicus Curiae Supporting Appellant, G.D. v. Kenny, 205 N.J. 275 (2011) (No. 65366) (urging this Court to preserve the right of expungement to combat the risk that private firms will make inaccurate and incomplete data available); Brief for EPIC et al. as Amici Curiae Supporting Appellee, State v. Reid, 194 N.J. 386 (2008) (No. 60756) (urging this Court to recognize that users have a constitutionally protected privacy interest in the identifying information provided to Internet service providers).

[1] EPIC IPIOP Clerk Jessica Hui contributed to this brief.

EPIC has also participated as *amicus curiae* in many other jurisdictions. See, e.g., Brief for EPIC et al. as Amici Curiae Supporting Petitioner, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402) (arguing that technological changes since the era of analog phones justify departing from the third-party doctrine); Brief for EPIC et al. as Amicus Curiae Supporting Petitioner, Packingham v. North Carolina, 137 S. Ct 1730 (2017) (No. 15-1194) (arguing that the First Amendment protects the right to access speech from the privacy of a personal electronic device); Brief for EPIC et al. as Amici Curiae Supporting Petitioner, Riley v. California, 573 U.S. 373 (2014) (No. 13-132) (arguing that, because modern cell phone technology provides access to an extraordinary amount of personal data, a warrantless search of a person's cell phone is a substantial and unnecessary infringement of privacy); Brief for EPIC as Amicus Curiae Supporting Appellant, Jackson v. McCurry, 762 Fed. Appx. 919 (11th Cir. 2019) (No. 18-10231) (urging the court to limit searches of students' phones to "circumstances when it is strictly necessary" in light of Riley); Brief for EPIC as Amicus Curiae Supporting Appellant, United States v. Miller, No. 18-5578 (6th Cir. filed Oct. 17, 2018) (arguing that, because the Government could not establish the reliability of Google's email screening technique, its use constituted an unreasonable search); Brief for EPIC et al. as

Amici Curiae Supporting Defendant, Apple v. FBI, No. 16-10, 2016 WL 618401 (C.D. Cal. 2016) (arguing that forcing Apple to redesign iPhones to enable law enforcement access "places at risk millions of cell phone users across the United States").

PRELIMINARY STATEMENT

The U.S. Supreme Court has recognized that the vast amount of personal information modern cell phones store, access, and generate justifies strong constitutional protections. In Riley v. California, 573 U.S. 373 (2014), and Carpenter v. United States, 138 S. Ct. 2206 (2018), the Court refused to extend exceptions to the Fourth Amendment warrant requirement that were conceived before the present digital moment, when cell phones now give law enforcement easy access to "a cache of sensitive personal information." Riley, 573 U.S. at 395. The Court decreed that courts are "obligated——as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government'——to ensure that the 'progress of science' does not erode" constitutional protections. Carpenter, 138 S. Ct. at 2223 (quoting Olmstead v. United States, 277 U.S. 438, 473–74 (1928)).

Similar to the search-incident-to-arrest and third-party exceptions to the Fourth Amendment warrant requirement at issue in Riley and Carpenter, the foregone conclusion exception to the Fifth Amendment was developed in an age dominated by physical,

not digital, evidence. In 1976, when the U.S. Supreme Court decided Fisher v. United States, 425 U.S. 391 (1976), introducing the foregone conclusion exception, cell phones did not exist. In 2000, when the Court last considered the exception in United States v. Hubbell, 530 U.S. 27 (2000), cell phones were still only mobile means for making telephone calls——not the "minicomputers" they are today. Riley, 573 U.S. at 393. Now, there are over 300 million cell phones, Pew Research Center, Mobile Fact Sheet (June 12, 2019),[2] with storage and data capacities that were "nearly inconceivable" in 2000. Riley, 573 U.S. at 385.

Since Hubbell, some courts——including the court below——have only required the Government to demonstrate knowledge of the existence, the target's possession, and the authenticity of a cell phone passcode to gain access to a device under the foregone conclusion exception. This broad interpretation of the exception places an astonishing amount of sensitive data in the hands of law enforcement through coercion of the suspect, in sharp contradiction to the reasons underlying the Fifth Amendment privilege against self-incrimination.

The U.S. Supreme Court's decisions in Riley and Carpenter counsel a different approach. Indeed, other courts have

[2] https://www.pewinternet.org/fact-sheet/mobile/.

acknowledged that "[t]he considerations informing the Court's Fourth Amendment analysis of a cell phone's role in modern day life, we believe raise Fifth Amendment concerns as well." In re Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017). The lower court's interpretation of the foregone conclusion exception should be rejected in favor of an approach that requires the Government to demonstrate actual knowledge pertaining to the information it wishes to access through the cell phone.

ARGUMENT

I. Cell phones provide access to a vast amount of information that law enforcement previously had to expend substantial resources to identify and locate.

Modern cell phones have fundamentally changed the scope of personal information available to law enforcement agencies pursuant to a search. As Chief Justice Roberts wrote in Riley, "[t]he term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone." 573 U.S. at 393. From bank records to medical records to photos, videos, and internet browsing history, Americans' cell phones are a window into their personal lives. In the past, law enforcement had to expend a great deal of effort to obtain evidence detailing every facet of a person's life. But today, "a digital record of nearly every

aspect of [Americans'] lives" is accessible by inputting one numerical or biometric passcode. Id. at 375.

Smartphones are ubiquitous; 81% of Americans own one. Pew Research Center, Mobile Fact Sheet (June 12, 2019).[3] Chief Justice Roberts noted that the devices "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude that they were an important feature of the human anatomy." Riley, 573 U.S. at 385.

In Riley, Chief Justice Roberts explained that "[c]ell phones differ in both a quantitative and a qualitative sense" from non-digital objects. 573 U.S. at 393. The Chief Justice wrote that "[o]ne of the most notable distinguishing features of modern cell phones is their immense storage capacity." Id. In 2014, when Riley was decided, the top-selling smartphone had "a standard capacity of 16 gigabytes . . .[, which] translates to millions of pages of text, thousands of pictures, or hundreds of videos." Riley, 573 U.S. at 394. Today, the average phone has a storage capacity of 64GB. Andrew Martonik, Let's Be Honest, 64GB of Internal Storage is Plenty in 2018, Android Central (Feb. 2, 2018).[4] That is over 1 million word documents, 200,000 PDF documents, almost 40,000 photos, 42 full length movies, and

[3] https://www.pewinternet.org/fact-sheet/mobile/.
[4] https://www.androidcentral.com/64gb-internal-storage-plenty.

almost 15,000 songs. iClick, How Big is a Gig? (2013).[5] Cell phone storage continues to grow. Apple sells 256GB iPhones and 512GB iPads. Apple, About Storage on Your Device and in iCloud (Sep. 27, 2018).[6] Samsung is allegedly developing a 1TB storage chip for cell phones. Sam Byford, Samsung is Making 1TB Storage Chips for Phones, The Verge (Jan. 30, 2019).[7] Cell phone capacity is extended even further by "cloud computing" and other remote access tools that allow users to "access data located elsewhere, at the tap of a screen." Riley, 573 U.S. at 397.

The average American adult spends an average of 226 minutes on their cell phone a day and uses their cell phones to complete a wide range of tasks. See Ethan Jakob Craft & George P. Slefo, Mary Meeker's 2019 Internet Trends Report, AdAge (June 11, 2019) [hereinafter Mary Meeker's Report].[8] The result is that cell phones have access to information and records relating to an astonishing amount of an individual's life. A cell phone "collects in one place many distinct types of information——an address, a note, a prescription, a bank statement, a video——that reveal much more in combination than any isolated record." Riley, 573 U.S. at 375. A phone's "capacity allows even just one

[5] https://www.iclick.com/pdf/howbigisagig.pdf.
[6] https://support.apple.com/en-us/HT206504.
[7] https://www.theverge.com/circuitbreaker/2019/1/30/18203347/samsung-1tb-flash-memory-eufs-phones-galaxy-s10.
[8] https://adage.com/article/digital/mary-meekers-2019-internet-trends-report-11-highlights-and-lots-industry-insight/2177626.

type of information to convey far more than previously possible" in part because "the data on a phone can date back to the purchase of the phone, or even earlier." Id. Further, while individual pieces of information may not themselves be incriminating, they could be if taken together. As Hal Abelson, Hen Ledeen, and Harry Lewis wrote: as technology gets "better and better at extracting meaning, . . . [it may] sometimes [] reveal things about us we did not expect others to know." Hal Abelson, Hen Ledeen, & Harry Lewis, Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion 2 (2008).

The average American has over 100 apps installed on their phone, App Annie, The State of Mobile 2019 at 13 (2019),[9] and accesses their apps 8.3 times a day, J. Clement, Average Daily Usage Frequency Per App in U.S. 2018, Statista (Aug. 14, 2018).[10] Time spent on mobile apps accounts for just under 90% of cell phone usage. Dave Chaffey, Mobile Marketing Statistics Compilation, Smart Insights (July 11, 2018).[11] In 2018, there were over 20 million registered app developers for iOS alone and some 500 million visitors to Apple's app store per week. Ingrid Lunden, App Store Hits 20M Registered Developers and $100B in

[9] Available at https://www.appannie.com/en/insights/market-data/the-state-of-mobile-2019/.
[10] https://www.statista.com/statistics/243856/daily-app-use-by-us-mobile-app-users/.
[11] https://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/.

Revenues, 500M Visitors Per Week, TechCrunch (June 4, 2018).[12] These apps "offer a range of tools for managing detailed information about all aspects of a person's life" that can "form a revealing montage of the user's life." Riley, 573 U.S. at 396. Almost 50% of mobile users use their phones to access their banks, credit union, or credit card. Caroline Cakebread, Who's Mobile Banking in the US?, eMarketer (Dec. 6, 2018).[13] Almost 60% of users have used one of the over 45,000 health-related mobile apps available. Paul Krebs & Dustin Duncan, Health App Use Among US Mobile Phone Owners: A National Survey, 3 JMIR mHealth and uHealth 101 (2015);[14] Matej Mikulic, Apple App Store: Number of Available Medical Apps as of Q1 2019, Statista (May 6, 2019).[15] Such apps capture and store very sensitive information. Apple's Health App, which is automatically installed on all iPhones, cannot be deleted and holds a cell phone owner's daily steps, meal habits, heart rate, reproductive health and sleep schedules, health records——including one's daily medication,

[12] https://techcrunch.com/2018/06/04/app-store-hits-20m-registered-developers-at-100b-in-revenues-500m-visitors-per-week/.
[13] https://www.emarketer.com/content/is-mobile-phone-banking-usage-near-saturation.
[14] Available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4704953/.
[15] https://www.statista.com/statistics/779910/health-apps-available-ios-worldwide/.

immunization records, clinical vitals——and more. Apple, Empower Your Patients with Health Records on iPhone (2019).[16]

Consumers also continue to use their phones as communication devices. As cell phone users turn away from phone calls and towards text messages and emails, cell phone data will increasingly track and memorialize all conversations. Already, Americans send texts and emails twice as often as they call. Irene Rufferty, 50 Texting Statistics That Can Quench Everyone's Curiosity, Even Mine, Medium (Sept. 20, 2017) [hereinafter 50 Texting Statistics].[17] Over 80% of Americans communicate by text every day. Id. In 2017, American cell phone users sent 2.27 trillion messages, around 45% of the entire world's text messaging volume. Id. Moreover, there are over 244.5 million email users in the United States, 72% of whom check their emails using their cell phones. J. Clement, E-Mail Usage in the United States, Statista (Oct. 23, 2018).[18] Notably, messaging platforms that offer encryption services, such as Telegram and Whatsapp, have outpaced the growth of non-encrypted messaging services, indicating the ever-increasing importance of personal privacy to

[16] https://www.apple.com/healthcare/health-records/.
[17] https://medium.com/bsg-sms/50-texting-statistics-that-can-quench-everyones-curiosity-even-mine-7591b61031f5.
[18] https://www.statista.com/topics/4295/e-mail-usage-in-the-united-states/.

consumers. Mary Meeker's Report. In 2018, 87% of web traffic was encrypted, up from 53% in 2016. Id.

Social media use is also proliferating: 73% of US adults use YouTube, 69% use Facebook, 37% use Instagram, and 24% use Snapchat. Andrew Perrin & Monica Anderson, Share of U.S. Adults Using Social Media, Including Facebook, Is Mostly Unchanged Since 2018, Pew Research Ctr. (Apr. 10, 2019).[19] For millennials, the numbers are even more striking: 91% use YouTube, 79% use Facebook, 67% use Instagram, and 62% use Snapchat. Id. Each app stores personal data, including search history, preferences, and more.

Cell phones do not just store personal data; they also contain sensitive business records. Almost 90% of companies expect their employees to use their cell phones for work purposes; 77% expect that percentage to increase within a year. Syntonic, BYOD Usage in the Enterprise (2016).[20] Just under 80% of American consumers text for business-related purposes. 50 Texting Statistics. Additionally, while in the past, many workers had separate personal and professional cell phones, this is no longer the case. Only 26% of companies provide employees

[19] https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/.
[20] https://syntonic.com/wp-content/uploads/2016/09/Syntonic-2016-BYOD-Usage-in-the-Enterprise.pdf.

with work phones. Steelcase, Engagement and the Global Workplace (2016).[21] In contrast, 72% have a bring-your-own-device policy and actively encourage their employees to use personal devices for work purposes. Diane Garey, BYOD and Mobile Security, Tenable (Apr. 5, 2016).[22] With one's phone, not only can employees access their emails and personal documents, but they can also access critical enterprise systems, employee contracts, local business files, and more. Apperian, Executive Enterprise Mobility Report (2016).[23] As companies continue to build internal company- or department-specific applications, as 45% of companies already have, the use of personal cell phones for work-related purposes will only grow. Id.

Law enforcement need not enter a specific app to view sensitive information on a phone. Push notifications——messages from apps that pop up on a cell phone screen automatically——can display sensitive personal information about communications, transactions, and other activities. Almost 45% of iPhone users

[21] http://cdn2.hubspot.net/hubfs/1822507/2016-WPR/Americas/Final_Digital_PDF.pdf.
[22] https://www.tenable.com/blog/byod-and-mobile-security-2016-spotlight-report-results.
[23] https://go.apperian.com/rs/300-EOJ-215/images/Apperian%202016%20Executive%20Enterprise%20Mobility%20Report_FINAL_20160216.pdf.

and over 90% of Android users have activated push notifications. Accengage, 2018 Push Notification Benchmark (2018).[24]

Smartphones not only store and provide access to a wealth of sensitive data, they also act as a key to access a user's many accounts——social media accounts, bank accounts, email accounts, and other profiles. For example, Apple built a password storage system into the iPhone. See Apple, Set Up iCloud Keychain (2019) ("iCloud Keychain remembers . . . your information——like your Safari usernames and passwords, credit cards, Wi-Fi passwords, and social log-ins——on any device that you approve.")[25] Some mobile apps also keep users logged in by default. Other apps provide storage of user login information for many sites and applications in one place. See, e.g., Dashlane, Features (2019);[26] Zoho Vault, Store and Organize Passwords (2019);[27] LastPass, LastPass Mobile (2019).[28] This means that a user's online identities are all easily accessible to anyone who has access to their phone.

Many applications have password saving features and generally, "by default, applications will store your passwords

[24] Available at https://www.accengage.com/benchmark-opt-in-and-reaction-rates-of-push-notifications-and-in-app-messages-for-mobile-apps-2018-edition/.
[25] https://support.apple.com/en-us/HT204085.
[26] https://www.dashlane.com/features.
[27] https://www.zoho.com/vault/online-password-manager-features.html.
[28] https://helpdesk.lastpass.com/lastpass-mobile/.

and never ask you for them again." Jonathan Garro, Unlock the Power of Your Mac's Keychain Utility, Tuts+ (Apr. 15, 2013).[29] For example, when a user logs into Facebook on their iPhone, the app will keep the user logged in by default and store the password information, sometimes even in plaintext. Zack Whittaker, Facebook Admits It Stored "Hundreds of Millions" of Account Passwords In Plaintext, TechCrunch (Mar. 21, 2019).[30] Some social media accounts, such as Twitter and Facebook, are even embedded into the phone software, requiring the user to take affirmative steps to log out. See Twitter, How to Log Out of the Twitter App on an iOS Device (2019);[31] Facebook, How do I Log Out of the iPhone or iPad App? (2019).[32]

In addition to storing passwords that provide access to a user's online accounts, smartphones also provide a mechanism to verify a user's identity. This type of authentication, commonly referred to as "two-factor authentication," is becoming standard for many online accounts. See Eric Griffith, Two-Factor

[29] https://computers.tutsplus.com/tutorials/unlock-the-power-of-your-macs-keychain-utility--mac-48730.
[30] https://techcrunch.com/2019/03/21/facebook-plaintext-passwords/.
[31] https://help.twitter.com/en/using-twitter/revoke-twitter-access-on-ios-app.
[32] https://www.facebook.com/help/ipad-app/112099682212213?helpref=uf_permalink.

Authentication: Who Has It and How to Set It Up, PCMag (Mar. 11, 2019).[33]

Smartphones can also control and monitor an individual's home. From one's cell phone, an individual can control the temperature of their apartment, turn on their lights, and can even view into their homes. See Google Nest Help, How to Control Your Nest Thermostat With the App (2019);[34] SmartHome, Control Lights With Your Phone (2019);[35] Apple, Set Up and Use the Home App (2019).[36] Companies have even begun offering digital door locks that can be unlocked using an iPhone or other mobile device. See John R. Delaney, The Best Smart Locks for 2019, PCMag (July 1, 2019);[37] Alexandra Chang, Your Door is About to Get Clever: 5 Smart Locks Compared, Wired (June 19, 2013).[38] Smartphones can similarly be used to deactivate a user's home security system, open their garage door, and control other home security features. See Alex Young, Can I Control My Home Security from My Phone, Safewise (May 17, 2019);[39] Kim Zetter,

[33] https://www.pcmag.com/feature/358289/two-factor-authentication-who-has-it-and-how-to-set-it-up.
[34] https://support.google.com/googlenest/answer/9249866?hl=en.
[35] https://www.smarthome.com/iphone_apps.html.
[36] https://support.apple.com/en-us/HT204893.
[37] https://www.pcmag.com/article/344336/the-best-smart-locks.
[38] https://www.wired.com/2013/06/smart-locks/.
[39] https://www.safewise.com/home-security-faq/home-security-phone/.

How Thieves Can Hack and Disable Your Home Alarm System, Wired (July 23, 2014).[40]

When law enforcement gains access to a smartphone, they are gaining access to every facet of a person's life. Because cell phones contain a vast amount of sensitive personal information, past court cases that permitted a defendant to be compelled to sign a disclosure authorization form (to gain access to particular financial records), Doe v. United States, 487 U.S. 201, 203 (1988), provide blood samples (to determine blood alcohol content at a particular moment in time), Schmerber v. California, 384 U.S. 757, 765 (1966), and to create a voice exemplar (to identify a voice on a tape), United States v. Dionisio, 410 U.S. 1, 7 (1973), are not apt analogies. As in Riley, the sweep of the possible search counsels against the extension of a pre-digital era exception.

II. Recent U.S. Supreme Court decisions concerning privacy protections for cell phones counsel in favor of a narrow application of the Fifth Amendment foregone conclusion exception.

In two recent decisions written by Chief Justice Roberts, the U.S. Supreme Court has established strong Fourth Amendment privacy protections for cell phones, and has declined to extend traditional exceptions that limited protection for physical objects. Both decisions were based on the "quantitative" and

[40] https://www.wired.com/2014/07/hacking-home-alarms/.

"qualitative" differences between the data stored on and generated by cell phones and the information contained in traditional physical objects and business records. Riley, 573 U.S. at 393. The Court sought to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." Carpenter, 138 S. Ct. at 2214 (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

The foregone conclusion exception to the Fifth Amendment privilege against self-incrimination was similarly formulated in the age before cell phones, when an individuals' documents of interest were not all consolidated in one place. Today, most of an individual's sensitive records are accessible through their cell phone, full access to which is guarded by a single passcode. Pre-digital antecedents, such as a safe or a lockbox, could not possibly hold as many documents or as much information about a person as their cell phone now does. As Chief Justice Roberts wrote, "a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—— unless the phone is." Riley, 572 U.S. at 396 (emphasis in original). Requiring the Government to only demonstrate knowledge of the existence, possession, and accuracy of a

passcode, as opposed to knowledge of the actual information the Government wishes to access from the cell phone, would allow the Government to go fishing in a gigabytes-deep sea of personal data.

A. In Riley v. California and Carpenter v. United States, the U.S. Supreme Court signaled that courts should preserve constitutional protections, and narrow exceptions, for cell phone data.

In Riley, the U.S. Supreme Court declined to extend the search-incident-to-arrest exception to the Fourth Amendment to cell phones. 573 U.S. at 386. In doing so, the Court rejected the claim that searches of cell phones were "materially indistinguishable" from searches of "other sorts of physical items." Id. at 393. Chief Justice Roberts likened the analogy to "saying a ride on a horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from Point A to Point B but little else justified lumping them together." Id. The Court explained that, while the exception "strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones." Id. at 386. That is because a "search of the information on a cell phone bears little resemblance to the type of brief physical search" that originated the exception." Id. Rather, the Court recognized that "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the

search of" non-digital objects, pointing, among other things, to the device's storage capacity and use for a wide range of tasks. Id. at 393. The Court stressed that "[t]he fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." Id. at 403.

Similarly, in Carpenter, the Court refused to extend the third-party doctrine to cell-site location information, explaining that "seismic shifts in digital technology" required a reconsideration of the doctrine as applied "to a distinct category of information:" cell phone data. 138 S. Ct. at 2219. The Court noted that, when the third-party doctrine was introduced in Smith v. Maryland, 442 U.S. 735 (1979), "few could have imagined a society in which a phone goes wherever its owner goes." 138 S. Ct. at 2217. In 1979, law enforcements' capabilities "were limited by a dearth of records and the frailties of recollection." Id. at 2218. As such, society expected that law enforcement agents could not "secretly monitor and catalogue [an individual's] every single movement." Id. at 2217 (citations omitted) .

However, in the digital age, providing law enforcement with access to an individual's cell phone data would "contravene[] that expectation" because cell phones provide "near perfect surveillance, as if [the Government] had attached an ankle

monitor to the phone's user." Id. at 2217–18. Because of a cell phone's ability to store vast amounts of data——providing detailed information of a user's present and past——phones are "unique," "qualitatively different," and do not "fit neatly under existing precedent[]." Id. at 2214, 2216–17. The Court recognized that "mechanical" application of the third-party doctrine to cell phone data would leave individuals "at the mercy of advancing technology" and would corrode constitutional values. Id. at 2214 (quoting Kyllo, 553 U.S. at 35) .

B. A broad interpretation of the foregone conclusion exception as applied to cell phones would significantly undermine Fifth Amendment protections.

The assessment of cell phone searches underlying Riley and Carpenter should be applied to the Fifth Amendment context. Indeed, the Supreme Court has recognized that "[t]he values protected by the Fourth Amendment . . . substantially overlap those the Fifth Amendment helps to protect." Schmerber, 384 U.S. at 767. Further, the Court has explained that "the gulf between physical predictability and digital capacity will only continue to widen in the future," Riley, 573 U.S. at 394, and the Court must adopt rules that "take account of more sophisticated systems that are already in use or in development," Carpenter, 138 S. Ct. at 2218-19 (quoting Kyllo, 533 U.S. at 36). Otherwise, a "mechanical interpretation" of the foregone

conclusion exception would leave individuals "at the mercy of advancing technology." Id. at 2214.

Similar to the exceptions at issue in Riley and Carpenter, the foregone conclusion exception was developed in a pre-digital age. The Fifth Amendment protects individuals from being "compelled in any criminal case to be a witness against himself." U.S. Const. amend. V. In 1966, decades before the invention of cell phones, the Court limited the Fifth Amendment to "compelling 'communication' or 'testimony,'" as opposed to "real or physical evidence." Schmerber, 384 U.S. at 764. The foregone conclusion exception followed in 1979: compelled information would not be "testimonial" for Fifth Amendment purposes if the information "adds little or nothing to the sum total of the Government's information." Fisher, 425 U.S. at 411. The Supreme Court last considered the exception in 2000, prior to the widespread use of the smartphone: production of documents is testimonial if production reveals (1) the existence of, (2) the defendant's possession of, and (3) the authenticity of the documents——but production is a "foregone conclusion" if the Government knows all three. Hubbell, 530 U.S. at 45.

In Hubbell, the Court found that the compelled production of 13,120 pages of materials was not a foregone conclusion but a "fishing expedition" because the demand "was tantamount to answering a series of interrogatories asking a witness to

disclose the existence and location of particular documents fitting certain broad descriptions." 530 U.S. at 41-42. Changes in technology have made it so that all 13,120 pages of production could now be stored or accessible from a single cell phone, protected by a single passcode. But under the lower court's test, the Government today could compel disclosure from Hubbell simply by demonstrating that knowledge of the existence of the passcode to his phone was a foregone conclusion, rather than having to prove knowledge of the existence on the phone of the actual documents at issue. That result——new technology giving law enforcement easy access to an extraordinary amount of personal information that would have previously infringed on an individuals' constitutional rights——is precisely what the Court in Riley and Carpenter stood against.

While the warrant in this case was limited to some extent, the court's reason for compelling the passcode from Appellant had nothing to do with any files the Government may have identified for production. Instead, the lower court only required a demonstration that the Government knew that the passcode existed, that Appellant possessed the passcode, and that the passcode was authentic——not that any of the information or documents the Government sought from the cell phone existed, or were in Appellant's possession, or were authentic. That rule will "prove no practical limit at all" to compelled decryption

of cell phones in New Jersey. Riley, 573 U.S. at 398. As Bruce Schneider and Orin Kerr argue, merely requiring knowledge of passwords is "vastly easier for the government to meet in practice because evidence that the person uses the phone regularly is likely sufficient to establish that the person knows the password." Bruce Schneider and Orin Kerr, Encryption Workarounds, 106 Geo. L.J. 989, 1003 (2018).

Indeed, courts that only require government knowledge that a password will unlock the device almost always find a foregone conclusion, see, e.g., Commonwealth v. Jones, 117 N.E. 3d 702, 718 (Mass. 2019); Commonwealth v. Davis, 176 A.3d 869, 876 (Pa. Super. Ct. 2017); United States v. Mitchell, 76 M.J. 413, 424 (C.A.A.F. 2017); State v. Stahl, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016); United States v. Fricosu, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012), whereas courts that require knowledge of particular files on the phone produce more mixed results depending on how well the Government has done its homework, see, e.g., United States v. Apple Mac Pro Computer, 851 F.3d 238, 247–48 (3d Cir. 2017) (holding that disclosure could be compelled because the Government proved the file's existence on the encrypted device); In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1337 (11th Cir. 2012) (requiring the Government to show that the drive "actually" contains useful files); G.A.Q.L. v. State, 257 So. 3d 1058, 1063

(Fla. Dist. Ct. App. 2018) (explaining that to require mere knowledge of passwords "would expand the contours of the foregone conclusion exception so as to swallow the protections of the Fifth Amendment" because "every password-protected phone would be subject to compelled unlocking"); Commonwealth v. Baust, 89 Va. Cir. 267, 271 (Va. Cir. Ct. 2014) (finding that neither the passcode nor the existence and location of the recording at issue were a foregone conclusion).

Some courts have already applied Riley in the Fifth Amendment context to cabin compelled disclosure of passcodes. In In re Application for a Search Warrant, the court, citing Riley, declared that "[t]he considerations informing the Court's Fourth Amendment analysis of a cell phone's role in modern day life, we believe raise Fifth Amendment concerns as well." 236 F. Supp. 3d at 1073. Though the Supreme Court held that fingerprinting was not testimonial in United States v. Wade, 388 U.S. 218, 223 (1967), the Northern District of Illinois refused to extend Wade to "forced fingerprinting to unlock an Apple electronic device." In re Application for a Search Warrant, 236 F. Supp. at 1073. Citing Riley, the court reasoned that "simple analogy that equates the limited protection afforded a fingerprint used for identification purposes to forced fingerprinting to unlock an Apple electronic device that potentially contains some of the most intimate details of an individual's life (and potentially

provides direct access to contraband) is supported by Fifth Amendment jurisprudence." Id. at 1073-74.

Similarly, in In re Search of a Residence in Oakland, 354 F. Supp. 3d. 1010 (N.D. Cal. 2019), the court recognized that, in light of Riley, cell phones "should be offered more protection" under the Fifth Amendment. Id. at 1017. Citing Riley and Carpenter, the Court declared that "[t]oday's mobile phones are not comparable to other storage equipment, be it physical or digital, and are entitled to greater privacy protection." Id. Quoting Riley, the court noted that in "the cell phone context . . . it is reasonable to expect that incriminating information will be found on a phone regardless of when the crime occurs." Id. (quoting Riley, 573 U.S. at 399). The court observed "that any argument that compelling a suspect to provide a biometric feature to access documents and data is synonymous with producing documents pursuant to a subpoena would fail. As the Riley court recognized, smartphones contain large amounts of data, including GPS location data and sensitive records, the full contents of which cannot be anticipated by law enforcement." Id. at 1018 (citing Riley, 573 U.S. at 399).

CONCLUSION

Amicus respectfully asks this Court to hold the foregone conclusion exception cannot justify the compelled disclosure of a cell phone passcode——and, thus, production of the contents of the

phone——merely upon demonstration that the passcode, and not the underlying records, is a foregone conclusion.

DATED:

FRANK L. CORRADO
(SBN 022221983)

BARRY, CORRADO, GRASSI &
GILLIN-SCHWARTZ, P.C.
2700 Pacific Avenue
Wildwood, NJ 08260
(609) 729-1333
fcorrado@capelegal.com

Alan Butler (*PHV Pending)
Megan Iorio (*PHV Pending)
ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Ave NW
Suite 200
Washington, DC 20009
(202) 483-1140